MARKED-UP VERSION

54. (Twice Amended) The computer readable medium according to claim 53, wherein the step of:

reencrypting the decrypted received content data with a local encrypting key includes encrypting with [IBM's]a SEAL algorithm.

74. (Twice Amended) The method according to claim 73, further comprising the step of:

decrypting the received previously encrypted content data prior to storage in the library;

reencrypting the decrypted received content data with a local encrypting key includes encrypting with [IBM's]a SEAL algorithm.

84. (Once Amended) The end user device according to claim 83, wherein the local encrypting key includes [IBM's]a SEAL algorithm.

Final Office Action Is Inappropriate In View of Newly Cited Art Ginter

Applicants have studied the Office Action dated March 15, 2002. Applicants respectfully request entry of these remarks under the provisions of 37 C.F.R. § 1.116(a) in that the remarks below place the application and claims in condition for allowance, which allowance is respectfully requested. Claims 53 - 62 and 73 - 87 are pending. Reconsideration and allowance of the claims in view of the following remarks are respectfully requested.

As an initial matter, the Examiner made the Office Action final based on a new ground of rejection not stated in the earlier Office Action. Applicants respectfully traverse this decision. In the Final Office Action, the Examiner rejects the present claims by citing Ginter (US 5,582,900), in view of Official Notice taken by the Examiner. The Applicants respectfully point out that the Ginter reference were not cited in any the previous Office Action.

According to MPEP § 706.07(a): "Under present practice, second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection not necessitated by amendment of the application by applicant, whether or not the prior art is already of record." In the previous Office Action dated September, 14, 1999 (Paper No. 5) , the Examiner examined the wrong claims since claims 1-44 were canceled by a preliminary amendment when this divisional application was initially filed. After a telephone interview with the Applicant's representative, the Examiner subsequently withdrew this Office Action on December 13, 1999. Next, in the first substantive office action dated July 27, 2001 (Paper No. 12), the Examiner rejected claims 53 - 62 and 73 - 82 under 35 U.S.C. § 102(e) as being anticipated by Ginter et al, (U.S. 5,892,170)[1]. In the previously-filed amendment, Applicants amended the independent claims 53, 73, and 83 for clarity and to include an additional limitation of "reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content." The Applicants did not

[1] It is important to note that the Ginter reference cited ((U.S. 5,892,170) is not the same Ginter reference of the final office action Ginter (U.S. 5,892,900).

switch from one subject matter to another or resort to any subterfuge to keep the application pending.[2] Thus it is respectfully submitted that the final status of the Office Action is premature and should be withdrawn.

If the Examiner does not withdraw the final status of the Office Action, Applicants submit that this response does not raise new issues in the application. It is submitted that the present response places the application in condition for allowance or, at least, presents the application in better form for appeal. Entry of the present response is therefore respectfully requested.

[2] See MPEP § 706.07.

REMARKS

Applicants have studied the Office Action dated Office Action dated March 15, 2002 and have made amendments to the claims. It is submitted that the application, as amended, is in condition for allowance. By virtue of this amendment, claims 53 - 62 and 73 - 87 are pending. Reconsideration and allowance of the pending claims in view of the above amendments and the following remarks are respectfully requested. In the Office Action, the Examiner:

- rejected claims 52, 74, and 84 under 35 U.S.C. § 112, second paragraph as being indefinite because they contain an IBM trademark; and
- rejected claims 53 - 62 and 73 - 87 under 35 U.S.C. § 103(a) as being unpatentable by Ginter et al, (U.S. 5,892,170), in view of Official Notice taken by Examiner.

Overview of the Current Invention

Preferred Embodiments of the present invention provide an improved method, apparatus and computer readable medium to manage electronic digital content on end-user devices. The present invention provides a set of tools that can handle the decryption of the digital content in a tamper resistant environment, that is, an environment to deter the unauthorized access to the content being played on an end user device. In addition, the present invention provides a local reencryption process that permits faster access to encrypted data and that permits the encrypted content to be deencrypted in a stream while playing. This is unlike the prior art systems that require the entire content to be decrypted prior to being played. This minimizes the exposure of decrypted content while the content is played because only a very small portion of the encrypted content is decrypted during playback. As stated in the specification o the present invention in the section entitled "C. Secure Container Processor 192" page 133 and more generally pages 131 - 135 (Emphasis added)

> "The process of Decryption and Re-Encryption 194 serves two purposes. Storing the Content 113 encrypted with an algorithm like SEAL enables faster than real-time decryption and requires much less processor utilization to perform the decryption than does a more industry standard type algorithm like DES. This enables the Player Application 195 to perform a real-time concurrent

decryption-decode-playback of the Content 113 while the encrypted content is being decrypted and without the need to first decrypt the entire file for the Content 113 prior to decode and playback. The efficiency of the SEAL algorithm and a highly efficient decode algorithm, allows not only concurrent operation (streaming playback from the encrypted file) but also allows this process to occur on a much lower powered system processor. Thus this application can be supported on a End-User Device(s) 109 as low end as a 60MHz Pentium system and perhaps lower. Separating the encryption format in which the Content 113 is finally stored from the original encryption format, allows for greater flexibility in the selection of the original content encryption algorithm. Thus use of widely accepted and proven industry standard algorithms can be used thus further enhancing Digital Content Industry acceptance of the Secure Digital Content Electronic Distribution System 100.

Unlike prior art systems the local reencrypting and encryption process uses a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content.

In order to more particularly point out these features of: a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content, the following language has been added the independent claims during the last office action, i.e., claims 53, 73, and 83 as follows [3]:

- Claims 53 and 73

  reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content;

---

[3] See §2173.05(i) Negative limitations in claims is not wrong so long as the boundaries of the patent protection sought are set forth definitely as they are here in the present invention.

- Claim 83

a software application for

decrypting the received previously encrypted content; and for

reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content;

Rejection under 35 U.S.C. §112, ¶2

As noted above, rejected claims 52, 74, and 84 under 35 U.S.C. § 112, second paragraph as being indefinite because they contain an IBM trademark under MPEP § 2173.05(u). Under MPEP § 2173.05(u) the use of a trademark is not *per se*, improper under 35 U.S.C. 112, second paragraph, and the use of "IBM" was to identify the source of the algorithm, not the algorithm themselves are proper under both trademark law and under MPEP 2173.05(u). However, for the purpose of expediting the patent application process in a manner consistent with PTO's Patent Business Goals (PBG),m 65 Fed. Reg. 54603 (September 8, 2000), the trademark has been removed so as to refer to a generic SEAL algorithm. Accordingly, the Applicants submit that the Examiner's rejection under 35 U.S.C. § 112, second paragraph, has been overcome and should be withdrawn.

Rejection under 35 U.S.C. §103(a)

As noted above, the Examiner rejected claims 53 - 62 and 73 - 87 under 35 U.S.C. § 103(a) as being unpatentable by Ginter et al, (U.S. 5,892,170), in view of Official Notice taken by Examiner. The Applicants respectfully travers this rejection. The Examiner at page 4 of the office action states *"Regarding claim 73, Ginter discloses [...] decrypting each content data selected to be played with its unique decrypting key, wherein the decrypting is performed in a tamper-resistant subroutine for deterring unauthorized access to the instructions for decrypting the content data and for deterring unauthorized access to the decrypting key (column 195, lines 27-47 and column 64,*

line 15-40) [...]" The Applicants respectfully traverse this argument. Careful reading of Ginter at Col. 64, line 16 describes a hardware package as the security barrier. This hardware barrier requires any machine using the solution proposed as taught by Ginter to have this specialized SPU 500 hardware device. In contrast, the present invention uses a "tamper resistant" environment that is completely built as part of the application so as to eliminate the need of additional hardware costs as taught by Ginter. Each independent claim in the present invention particularly points out and distinctly claims a "tamper resistant environment" that does not rely on specialized hardware of Ginter:

> wherein the decrypting is performed in a tamper-resistant subroutine for deterring unauthorized access to the instructions for decrypting the content data and for deterring unauthorized access to the decryption key;

This is an important distinction since unlike the present invention, Ginter teaches and describes the use of the specialized hardware and therefore the solution of Ginter will not work on all the installed base of commercially available PC's without additional hardware.

The Federal Circuit has consistently held that when a §103 rejection is based upon a modification of a reference that destroys the intent, purpose or function of the invention disclosed in the reference, such as proposed modification is not proper and the *prima facie* case of obviousness can not be properly made. See In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Here the solution taught by Ginter can not operate on commercially available PCs without hardware modifications to include the specialized SPU 500 hardware. Because Ginter does not provide "a tamper-resistant subroutine for deterring unauthorized access to the instructions for decrypting the content data," this combination as suggested by the Examiner destroys the intent and purpose of the present invention of working on commercially available PCs without hardware modifications. Accordingly, the present invention is distinguishable over Ginter for at least this reason.

The Examiner at pages 4 and 3 of the office action continues and correctly states *"Regarding claim 73, Ginter does not discloses re-encypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encrypting key which enables streaming*

playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content. The Examiner goes on to take Official Notice that *"using stream encryption algorithm (SEAL) in which the local encrypting key is a type of encrypting key which enables streaming playback of the encrypted content while the encrypted content is being decrypted to encrypt the content is old and well-known in the art of cryptography. Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to implement the encryption method of Ginter's using stream encryption (SEAL) instead of data encryption algorithm DES) for the purpose of allowing [s]treaming (sic) playback of encrypted content."* To begin, under MPEP § 2144.03, where the Examiner takes official notice on facts outside the record and "when a rejection is based on facts within the personal knowledge" of the Examiner the Applicant may require an affidavit from the Examiner to support such personal knowledge. The Applicants respectfully request such an affidavit be submitted by the Examiner to put these facts on the record under MPEP § 2144.03.

Continuing further, when there is no suggestion or teaching in the prior art for using "local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted the suggestion can not come from the Applicants' own specification. As the Federal Circuit has repeatedly warned against using the Applicants' disclosure as a blueprint to reconstruct the claimed invention out of isolated teachings of the prior art. See MPEP §2143 and Grain Processing Corp. v. American Maize-Products, 840 F.2d 902, 907, 5 USPQ2d 1788 1792 (Fed. Cir. 1988) and In re Fitch, 972 F.2d 160, 12 USPQ2d 1780, 1783 84 (Fed. Cir. 1992). The prior art reference Ginter does not even suggest, teach nor mention "local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted."

Very recently, the Federal Circuit again took up the identical question of obviousness in combining references in the case In re Sang Su Lee, No. 00-1158 (January 18, 2002). In this case Board of Patent Appeals rejected all of Applicant's pending claims as obvious under § 103. The Federal Circuit vacated and remanded. Citing two prior art references, the Board stated that a person

of ordinary skill in the art would have been motivated to combine the references based on "common knowledge" and "common sense", but it did not present any specific source or evidence in the art that would have otherwise suggested the combination. The Federal Circuit held that the Board's rejection of a need for any specific hint or suggestion in the art to combine the references was both legal error and arbitrary agency action subject to being set aside by the court under the Administrative Procedure Act (APA). Accordingly, because there is no suggestion or motivation found in Ginter taken alone or in view of Official Notice, the Examiner has failed to properly establish a *prima facie* case of obviousness for the invention as a "whole." The Applicants submit the present invention distinguishes over Ginter for at least this reason as well.

Continuing, still further, careful reading of Ginter discloses reencrypting the entire item in the database. Or in the words of Ginter: "The keys to decrypt secure database 610 records are, in the preferred embodiment, maintained solely within the protected memory of an SPU 500. Each index or record update that leaves the SPU 500 may be time stamped, and then encrypted with a unique key that is determined by the SPE 503." See Ginter at Col. 171 lines 14-16 and FIG. 37. This is not the same as using reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content.[4] In fact, Ginter teaches exactly the problem in the prior art of decrypting and reencrypting using DES type keys and the use of proprietary hardware for a tamper resistant environment. See Ginter FIG. 6 and Col. 22, Lines 1 -14. The present invention provides reencrypting with an efficient algorithm, such as IBM's SEAL algorithm, and a highly efficient decode algorithm. Using this type of encryption and corresponding decryption, permits the present invention to concurrently operate (streaming playback from the encrypted file) and moreover provides a decryption system which is able to operate on a lower-powered system (i.e., lower processor power) without the use of specialized hardware such as the secure processing environment (SPE) 503 of Ginter. This is important because the present invention enables an encrypted playback

[4] See §2173.05(i) Negative limitations in claims is not wrong so long as the boundaries of the patent protection sought are set forth definitely as they are here in the present invention.

solution to scale from low-power end-user systems, such as Palm Pilot, up through higher power desktop systems. See Present Invention as entitled "C. Secure Container Processor 192" pages 133 (Emphasis added). Moreover, the present invention further provides greater flexibility by allowing for one type of encryption, such as DES, to be used when transmitting and receiving the encrypted content to the end-user device and another type of encryption to be used on low-powered devices to enable concurrent decryption and playback. Accordingly, the present invention independent claims 53, 73, and 84 distinguishes over Ginter for at least this reason, as well

The Examiner recites 35 U.S.C. §103. The Statute expressly requires that obviousness or non-obviousness be determined for the claimed subject matter "as a whole," and the key to proper determination of the differences between the prior art and the present invention is giving full recognition to the invention "as a whole." The Ginter reference taken alone or in view of Official Notice simply does not suggest, teach or disclose the patentably distinct limitations of:

> reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content;
>
> wherein the decrypting is performed in a tamper-resistant subroutine for deterring unauthorized access to the instructions for decrypting the content data and for deterring unauthorized access to the decryption key.

Independent claims 53, 73, and 83 as discussed above distinguish over Ginter taken alone or in view of Official Notice. Claims 54 - 62, 74 - 83, and 85 - 87, depend from claims 53, 73, and 83 respectively and since dependent claims contain all the limitations of the independent claims, claims 53-62, and 74 - 87 distinguish over Ginter alone or in view of Official Notice, as well.

CONCLUSION

In view of the foregoing, Applicants respectfully submits that all of the grounds for rejection stated in the Examiner's office action have been overcome, and that all claims in the application are allowable. No new matter has been added. It is believed that the application is now in condition for allowance, which allowance is respectfully requested.

PLEASE CALL the undersigned if that would expedite the prosecution of this application.

Respectfully submitted.

By: _____

Jon Gibbons (Reg. No. 37.333)
Attorney for Applicant
Fleit, Kain, Gibbons, Gutman & Bongini, P.L.
One Boca Commerce Center, Suite 111
551 N.W. 77th Street
Boca Raton, FL 33487
Tel. (561) 989-9811
Fax (561) 989-9812

PLEASE Direct All Correspondence to Customer Number 23334

150-a99-062amend2.wpd